IN THE CLAIMS

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please ADD new claims in accordance with the following:

1. (Previously Presented) A security management device including:

a security detection unit detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;

a judging unit judging whether the security level of the user apparatus reaches a predetermined security level; and

an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network by the user apparatus.

2. (Previously Presented) A security management device according to Claim 1, wherein the access control unit, in case the judging unit judges that the security level of the user apparatus reaches the predetermined level, sets a range wider than the restriction range as the access permission range of the user apparatus.

3. (Previously Presented) A security management device according to Claim 1, wherein the access control unit has a function of controlling a communication route of the user apparatus and, in case the judging unit judges that the security level of the user apparatus does not reach the predetermined level, controls a communication destination of the user apparatus to a specified device in the restriction range on the network.

4. (Previously Presented) A security management device according to Claim 3, wherein the specified device controls updating the virus definition file of the user apparatus.

5. (Previously Presented) A method of managing computer security comprising:

detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;

judging whether the security level of the user apparatus reaches a predetermined security level; and

in case of judging the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network of the user apparatus.

6. (Previously Presented) A security management method according to Claim 5, wherein in case of judging the security level of the user apparatus reaches the predetermined level, setting a range wider than the restriction range as the access permission range of the user apparatus.

7. (Previously Presented) A security management method according to Claim 5, wherein in case of judging the security level of the user apparatus does not reach the predetermined level, the restricting of the access permission range of the user apparatus comprises changing a communication destination of the user apparatus to a specified device on the network.

8. (Previously Presented) A security management method according to Claim 7, wherein the specified device controls updating the virus definition file of the user apparatus.

9. (Previously Presented) A recording medium recorded with a security management program for making a computer execute:

detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;

judging whether the security level of the user apparatus reaches a predetermined security level; and

in case of judging the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network of the user apparatus.

10. (Previously Presented) A recording medium recorded with a security management program according to Claim 9, wherein in case of judging the security level of the user apparatus reaches the predetermined security level, setting a range wider than the restriction range as the access permission range of the user apparatus.

11. (Previously Presented) A recording medium recorded with a security management program according to Claim 9, wherein in case of judging the security level of the user apparatus does not reach the predetermined security level, the restricting of the access permission range of the user apparatus comprises changing a communication destination of the user apparatus to a specified device on the network.

12. (Previously Presented) A recording medium recorded with a security management program according to Claim 11, wherein the specified device controls updating the virus definition file of the user apparatus.

13. (Previously Presented) A security management system comprising:

a security management device, an apparatus for a user and a security setting guide device in communication via a network,

wherein the security management device comprises:

a security detection unit detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;

a judging unit judging whether the security level of the user apparatus reaches a predetermined security level; and

an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network by the user apparatus.

14. (Previously Presented) A security management system according to Claim 13, wherein the access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, connects the user apparatus to the security setting guide device.

15. (Previously Presented) A security management device including:

a controller

determining a security level of a user terminal upon a network access for the user terminal, based upon one or more of security information updating history of the user apparatus, port access information of the user terminal, or programs and/or scripts downloaded and/or executable at the user terminal, and

ensuring a predetermined security level on the network, according to the determined security level of the user terminal.

16. (Previously Presented) The security management device of claim 15, wherein the security information comprises a virus definition file and the security information updating history of the user terminal comprises an access pattern to a security information server for updating the security information and/or an access history to the security information server for updating the security information.

17. (Previously Presented) The security management device of claim 15, wherein the ensuring of the predetermined security level on the network comprises guiding the user terminal to meet the predetermined security level.

18. (Previously Presented) The security management device of claim 15, wherein the ensuring of the predetermined security level on the network comprises if the security level of the user terminal does not reach the predetermined security level, restricting an access permission range on the network of the user terminal.

19. (New) The security management device according to Claim 1, wherein the user apparatus is established to afford the network.

20. (New) The security management device according to claim 1, wherein the access control unit, in case the judging unit judges that the security level of the user apparatus has reached the predetermined security level, dose not restrict the access permission range on the network by the user apparatus.

21. (New) The security management method according to Claim 5, wherein the user apparatus is established to afford the network.

22. (New) The security management method according to claim 5, wherein in the case when it is judged that the security level of the user apparatus has reached the predetermined security level, the access permission range on the network by the user apparatus is not restricted.

23. (New) The security management system according to Claim 13, wherein the user apparatus is established to afford the network.

24. (New) The security management system according to claim 13, wherein the access control unit of the security management system, in case the judging unit judges that the security level of the user apparatus has reached the predetermined security level, dose not restrict the access permission range on the network by the user apparatus.

25. (New) The security management device according to Claim 15, wherein the user apparatus is established to afford the network.

26. (New) The security management device according to claim 1, wherein the controller, when determined by the ensuring that the security level of the user apparatus has reached the predetermined security level, does not restrict an access permission range on the network by the user apparatus.

27. (New) A method of managing security of a computer network to which a user terminal is communicably connected, comprising:

determining a security level of the user terminal upon access to the network from the user terminal, based upon security information updating history of the user apparatus, port access information of the user terminal, programs and/or scripts downloaded and/or executable at the user terminal, or any combinations thereof and

ensuring a security level on the network, according to the determined security level of the user terminal.